МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
Одеський державний університет внутрішніх справ

ПРАВОВЕ РЕГУЛЮВАННЯ ДОТРИМАННЯ ПРАВ І СВОБОД ЛЮДИНИ ТА ГРОМАДЯНИНА В УМОВАХ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ

Колективна монографія

За загальною редакцією
А. В. Денисової

Видавництво
«Юридика»
2025

УДК 342.7:351.86"364"(477)
П68

Рецензенти:

Журавльов Дмитро Володимирович, заступник керівника Департаменту з питань громадянства, помилування, державних нагород — керівник управління з питань помилування Офісу Президента України, доктор юридичних наук, професор;

Катеринчук Іван Петрович, професор кафедри вогневої підготовки ОДУВС, доктор юридичних наук, професор;

Гаран Ольга Володимирівна, професор кафедри адміністративного права та господарського права Одеського національного університету імені І. І. Мечникова, доктор юридичних наук, професор

Рекомендовано до друку Вченою радою
Одеського державного університету внутрішніх справ
(протокол № 12 від 30 вересня 2025 року)

П68 **Правове** регулювання дотримання прав і свобод людини та громадянина в умовах адміністративно-правового режиму воєнного стану : колективна монографія / Є. Львова, О. Жильцов, О. Пасько та ін. ; за заг. ред. А. В. Денисової. – Одеса : Видавництво «Юридика», 2025. – 840 с.

ISBN 978-617-8574-56-7

Колективна монографія присвячена комплексному аналізу правового регулювання дотримання прав і свобод людини в умовах воєнного стану в Україні. У виданні осмислено трансформацію механізмів їх забезпечення з урахуванням викликів збройної агресії. Досліджено реалізацію державної політики у гуманітарній, безпековій, правоохоронній, судовій і соціальній сферах, проблеми захисту прав дітей, цивільного населення, військовополонених, а також питання інформаційної безпеки та OSINT. Монографія адресована науковцям, юристам і практикам.

УДК 342.7:351.86"364"(477)

ISBN 978-617-8574-56-7

Зміст

DOI: 10.61563/978-617-8574-56-7-19

Розділ 19
OSINT ТА ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ВОЄННОГО СТАНУ

Наталія СВИРИДЮК
Одеський державний університет внутрішніх справ, Україна
ORCID 0000-0001-9772-1119

Дмитро АФОНІН
Одеський державний університет внутрішніх справ, Україна
ORCID 0000-0002-0951-7968

Вступ

Наше сьогодення характеризується стрімким розвитком цифрових технологій, які суттєво трансформували як природу сучасних міжнародних конфліктів, так і характер загроз національній та міжнародній безпеці. Зростання відкритості суспільств, розширення доступу до інформаційних ресурсів, а також глобалізація обміну даними зумовили формування нової аналітичної парадигми, у межах якої відкриті джерела інформації набули виняткового значення. Водночас цифровізація суспільства радикально змінила підходи до ведення воєнних конфліктів і зумовила появу нових засобів інформаційного впливу. У цьому контексті особливого значення набуває OSINT (Open Source Intelligence — розвідка з відкритих джерел), який став вагомим інструментом не лише у військово-стратегічному вимірі, але й у політичному, соціальному та правовому контекстах. В умовах зростання гібридних загроз та інтенсивного інформаційного протистояння OSINT поступово перетворюється на критичний компонент безпекової стратегії[1].

[1] Rid, T. (2020). Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux;

Zegart, A. (2022). Spies, Lies, and Algorithms: The History and Future of American Intelligence. Princeton University Press.

OSINT охоплює процес збору, аналізу та інтерпретації інформації з відкритих джерел, що не потребує спеціального доступу чи технічних засобів збору розвідувальних даних (наприклад, прослуховування або перехоплення)[2]. Йдеться про такі відкриті джерела, як офіційні вебсайти, соціальні мережі, форуми, медіаплатформи, бази даних, наукові публікації, державні реєстри, супутникові знімки тощо[3]. На відміну від традиційних форм розвідки таких як HUMINT (агентурна розвідка) чи SIGINT (технічна розвідка), OSINT базується на публічно доступній інформації, що дозволяє використовувати її не лише органами державної влади, а й відкриває можливість використання зазначеного інструменту й широкому колу осіб: представникам громадянського суспільства, науковцям, дослідникам, журналістам, правоохоронним структурам, військовим, волонтерам і навіть приватним особам.

Під час повномасштабного вторгнення росії в Україну у 2022 році значущість та роль OSINT значно зросла. Розвідка з відкритих джерел дозволила оперативно верифікувати атаки, документувати воєнні злочини, фіксувати переміщення військових підрозділів, ідентифікувати логістичні маршрути, а також OSINT забезпечує можливість отримання оперативних даних щодо морально-психологічного стану цивільного населення та військовослужбовців, рівня інфраструктурних втрат, актуальних гуманітарних потреб тощо. У багатьох випадках інформація з відкритих джерел забезпечувала точнішу картину, ніж традиційні розвідувальні методи, завдяки швидкості її поширення та колективному аналізу.

При цьому OSINT не вимагає суттєвих фінансових витрат або застосування високотехнологічних засобів, а базується переважно на аналітичних навичках і здібностях, критичному мисленні та системному підході аналітика. Зокрема, у ході війни в Україні

---

[2] Steele, R.D. (2007). Chapter: Open Source Intelligence. In: Loch Johnson (Ed.), Handbook of Intelligence Studies. Routledge.

[3] Open-Source Intelligence & its Legal and Ethical Aspects (July 25, 2024). URL: https://eithos.eu/open-source-intelligence-osint-its-legal-and-ethical-aspects

OSINT став ефективним інструментом численних виявлень воєнних злочинів та дезінформаційних кампаній, фіксації наслідків ракетних атак тощо.

Водночас, попри численні переваги, активне використання відкритих джерел в умовах збройної агресії несе серйозні виклики та супроводжується суттєвими ризиками для інформаційної безпеки.

Зокрема, на перший погляд дані, що здаються невинними (наприклад, зображення з геолокацією чи публікації у соціальних мережах), можуть неусвідомлено розкривати важливу інформацію стратегічного значення: точне розташування військових підрозділів, логістичні маршрути, стан об'єктів критичної інфраструктури.

Більше того, ворог також активно використовує відкриті джерела для реалізації елементів гібридної війни, зокрема для збору розвідданих, виявлення вразливостей, здійснення інформаційно-психологічних операцій і поширення фейкової інформації та маніпулювання громадською думкою з метою дестабілізації внутрішньої ситуації та розпалювання паніки серед населення. Відсутність належної цифрової гігієни серед користувачів підвищує вразливість критичної інфраструктури та безпеки військових операцій.

Особливістю OSINT є його двоспрямований характер. З одного боку, він слугує інструментом прозорості, підзвітності та підвищення ефективності аналітичної діяльності. З іншого — створює загрозу витоку конфіденційної або стратегічної інформації, якщо його використання не врегульоване або недостатньо контрольоване. Це зумовлює необхідність активної участі держави в регулюванні практик OSINT як через законодавчу нормалізацію, так і через формування культури інформаційної обережності серед громадян, розвиток аналітичних структур і забезпечення міжвідомчої взаємодії.[4]

[4] Steele, R.D. (2007). Chapter: Open Source Intelligence. In: Loch Johnson (Ed.), Handbook of Intelligence Studies. Routledge

Окрему увагу слід приділяти юридичному та етичному вимірам OSINT. Особливо у період воєнного стану виникає складний баланс між правом громадян на доступ до інформації та потребою забезпечення безпеки. Волонтери, журналісти або активісти, маючи намір сприяти суспільному контролю, іноді не усвідомлено розкривають критичну інформацію, яка може бути використана ворогом. Так само, у межах правового поля залишаються не завжди чітко та до кінця визначеними такі питання, як обсяг допустимого використання персональних даних, захист приватності, авторські права на зібрані матеріали. Це особливо актуально в умовах воєнного стану, де звичайні правові механізми можуть бути обмежені.

Разом з тим OSINT відкриває нові можливості для громадянського суспільства, правозахисників та міжнародних організацій. Під час війни в Україні відкриті джерела були використані для документування атак на цивільну інфраструктуру, верифікації злочинів проти людяності та ідентифікації ймовірних воєнних злочинців. Зібрані таким чином докази вже визнаються судами, зокрема Міжнародним кримінальним судом, використовуються у кримінальних провадженнях і відіграють критичну роль у майбутніх процесах притягнення до відповідальності за воєнні злочини.[5]

Окремо варто відзначити роль громадян у створенні OSINT-контенту. У сучасному середовищі будь-який користувач смартфону може виступати як джерело OSINT-даних. Фото з місця обстрілу або пошкодженої техніки, відео з місця події чи дрона, коментар або допис у Telegram-каналі можуть мати стратегічну цінність. Це вимагає широкомасштабної просвітницької кампанії щодо інформаційної гігієни та відповідальності, зокрема серед населення, яке перебуває у прифронтових регіонах.

Ефективність OSINT значною мірою залежить від його інтеграції в ширшу систему національної безпеки, кіберзахисту

[5] Bellingcat (2022). Investigations Archive. URL: https://www.bellingcat.com;
ICC (2023). Evidence from Open Sources in War Crimes Cases. International Criminal Court Briefing Paper.

та антикризового управління. Розвідка з відкритих джерел не повинна існувати ізольовано — вона має бути частиною загальної системи ситуаційного аналізу, оперативного реагування, інформаційного прогнозування. В Україні вже існують приклади успішної імплементації OSINT-підходів зокрема у діяльність ЗСУ, СБУ, кіберполіції та інших відомств. Необхідною умовою подальшого розвитку є міжвідомча координація, розвиток аналітичних центрів, формування міждисциплінарних команд (залучення фахівців з IT, соціології, лінгвістики, криміналістики та права) і технологічне забезпечення процесу обробки великих масивів відкритих даних[6].

Таким чином, об'єктивна необхідність системного аналізу OSINT в умовах воєнного стану випливає з поєднання таких чинників:

– стратегічна цінність відкритої інформації для державного та громадського секторів;

– зростаючі загрози, пов'язані з неконтрольованим поширенням чутливої інформації;

– потреба у розробці збалансованої політики регулювання, яка забезпечить ефективність і безпеку.

У цьому контексті, коли інформаційний фронт стає не менш важливим за фізичний, OSINT потребує системного осмислення та слід його розглядати не лише як технічний інструмент, а як багатовимірне соціально-політичне явище.

Саме тому актуальним є комплексне дослідження, спрямоване на систематизацію джерел OSINT; оцінку потенціалу та обмежень відкритої розвідки; аналіз практик використання OSINT у сфері безпеки; виявлення загроз інформаційній безпеці, а також формування пропозицій щодо правового, організаційного та технологічного забезпечення OSINT в умовах воєнного стану, з урахуванням українського досвіду, міжнародних практик та актуального безпекового контексту.

[6] UNIDIR (2022). Open Source Intelligence for Arms Control Verification. United Nations Institute for Disarmament Research.

OSINT як інструмент сучасної розвідки і безпеки

У сучасному світі розвідка з відкритих джерел є не лише важливим доповненням до традиційних форм здобуття розвідувальної інформації, а й самостійним інструментом стратегічного аналізу, прогнозування та інформаційного впливу. Зростання значущості OSINT є наслідком цифровізації, глобального поширення соціальних мереж, відкритості державних ресурсів, комерційної доступності супутникових даних і розвитку технологій автоматизованого аналізу великих масивів інформації[7].

Як зазначалося вище OSINT охоплює широкий спектр джерел: офіційні повідомлення, новинні ресурси, вебсайти державних установ, корпоративну звітність, бази даних реєстрів, акаунти в соціальних мережах, відео- та фотоматеріали, форуми, блоги, супутникові знімки, ресурси даркнету, картографічні сервіси тощо. Важливо, що ці дані зазвичай доступні без спеціальних технічних засобів, що забезпечує законність збору інформації, з одного боку, та її масовість — з іншого.

У даному контексті важливо зауважити, що у воєнних умовах OSINT виконує низку критичних функцій таких як:

Оперативна обізнаність. Інформація з відкритих джерел дозволяє в режимі реального часу отримувати відомості про ситуацію на фронті, наслідки обстрілів, переміщення техніки, ідентифікації особового складу, настрої в тилу та окупованих територіях, а також створення геоінформаційних платформ. У даному контексті наведемо приклади використання інформації з відкритих джерел. Наприклад, дані з Twitter, Telegram, TikTok, супутникових знімків або Google Maps можуть забезпечити швидку оцінку ситуації в регіоні бойових дій.[8]

---

[7] Baffa, Richard. The Ukraine-Russia War Confirms the Value of OSINT. URL: https://www.babelstreet.com/blog/the-ukraine-russia-war-confirms-the-value-of-osint

[8] The Role of OSINT in the Russia-Ukraine Conflict. Flashpoint. URL: https://www.flashpoint.io/resources/report/role-of-osint-russia-invasion-of-ukraine

Верифікація подій. OSINT дозволяє перевіряти правдивість заяв сторін конфлікту, ідентифікувати фейки, розпізнавати спроби дезінформації. Пошук метаданих у фото, зворотний пошук зображень або відео, геолокація об'єктів на картах — стандартна методика цифрової криміналістики, що використовується у OSINT.

Документування воєнних злочинів. Відкриті джерела стали одним з основних способів документування знищення цивільної інфраструктури, загибелі мирних жителів, порушення міжнародного гуманітарного права[9]. Багато правозахисних організацій — наприклад, Bellingcat[10], Forensic Architecture, OSINT Ukraine[11] — використовують відкриті дані для створення візуальних та хронологічних карт подій, які згодом стають доказами в судових процесах.[12]

Контррозвідка та інформаційна гігієна. OSINT дозволяє виявляти витоки конфіденційної інформації, оцінювати ступінь небезпеки від опублікованих матеріалів, формувати моделі інформаційної поведінки населення, виявляти підставні акаунти або ботоферми, ідентифікувати джерела поширення ворожої пропаганди.[13]

---

[9] Limonier, Kevin (2022). The war in Ukraine, open source investigation and the potential for «digital fieldwork» in geopolitics. URL: https://www.sciencedirect.com/science/article/am/pii/S0962629822001470;

Smith, Adam (2024). How Open Source Intelligence Can Help Prove War Crimes. Context News. URL: https://www.context.news/ai/how-can-open-source-intelligence-help-prove-war-crimes;

Ricci, Andrea and Crawford, Jack (2024). Puzzling Pieces: OSINT and War Crime Accountability in Ukraine. URL: https://rusi.org/explore-our-research/publications/commentary/puzzling-pieces-osint-and-war-crime-accountability-ukraine)

[10] Bellingcat. Guide: Online Investigation Tools and Techniques. URL: https://www.bellingcat.com/resources/how-tos/2021/09/14/bellingcat-online-investigation-toolkit

[11] OSINT for Ukraine. URL: https://osintforukraine.com/

[12] IWPR: Integrating OSINT into Justice Processes. URL: https://iwpr.net/global-voices/integrating-osint-justice-processes

[13] UK Cyber Security Council: Ethical Issues of OSINT. What is osint, and what ethical issues should be considered? URL: https://www.ukcybersecuritycouncil.org.uk/blogs/blogs/ethical-issues-of-osint

Підтримка операцій і планування. Аналітичні центри Збройних Сил, Служби безпеки, кіберполіції активно використовують OSINT для уточнення розвідувальних даних, оцінки ризиків при плануванні операцій, контролю за інфраструктурою ворога. Інформація з відкритих джерел може доповнювати або коригувати дані, отримані з HUMINT або SIGINT.[14]

Міжнародне партнерство та обмін даними. OSINT спрощує обмін інформацією з партнерами, оскільки не містить засекречених компонентів. Це пришвидшує спільне реагування на загрози, синхронізацію дій у межах багатонаціональних операцій, формування спільних баз даних воєнних злочинів.[15]

Використання технологій і методів OSINT під час воєнного стану здобуло значне поширення завдяки необхідності швидкого отримання інформації з відкритих джерел для оцінки ситуації, планування операцій та контррозвідки. Технологічні інструменти OSINT дозволяють військовим та розвідувальним службам швидко аналізувати великі обсяги інформації, що доступна через Інтернет та інші публічні канали.[16]

Нижче наведено деякі з найбільш поширених технологічних інструментів і методів OSINT, що використовуються в умовах війни.

Супутникові знімки та геопросторові технології. Супутникові знімки є одними з найбільш важливих інструментів OSINT під час конфліктів, оскільки вони надають детальну картину ситуації на місцевості. Військові та розвідувальні служби активно використовують доступні комерційні супутники, такі як Planet Labs, DigitalGlobe або Sentinel, для спостереження за переміщенням

[14] Schollaert, Kellen (2025). OSINT in Gray Zone Warfare. Penlink. URL: https://www.penlink.com/blog/osint-in-gray-zone-warfar

[15] Gauthier, David (2025). A Standalone OSINT Agency for Stronger National Security. The National Security Institute. URL: https://insideaipolicy.com/sites/insideaipolicy.com/files/documents/2025/feb/ai02032025.pdf

[16] Open-source intelligence in Ukraine: Asset or liability? URL: https://www.chathamhouse.org/2022/12/open-source-intelligence-ukraine-asset-or-liability?utm_source=chatgpt.com

військової техніки, рухом людських мас, будівельними роботами, пошкодженнями інфраструктури та іншими важливими аспектами, що можуть свідчити про військові операції.

Супутникові знімки допомагають у визначенні розташування та переміщення військових підрозділів і техніки; оцінці масштабів руйнувань інфраструктури внаслідок повітряних атак; виявленні нових об'єктів, що будуються (наприклад, військових баз або укриттів), а також аналізі логістичних шляхів та маршрутів постачання.

Для аналізу супутникових знімків використовуються спеціалізовані програми, такі як Google Earth або ArcGIS, а також більш складні рішення, що дозволяють виявляти аномалії, відслідковувати зміни з часом та здійснювати просторовий аналіз.

Соціальні мережі та інтернет-ресурси. Соціальні мережі, зокрема Twitter, Facebook, Instagram, Reddit та Telegram, є основним джерелом інформації в реальному часі, оскільки вони дозволяють отримати свіжі новини від місцевих жителів, журналістів, активістів і навіть учасників конфлікту. Під час війни, користувачі активно публікують відео, фотографії, геолокаційні дані, що дають можливість аналізувати ситуацію на місцях.

До основних методів аналізу інформації з соціальних мереж належать:

моніторинг хештегів і ключових слів: за допомогою спеціальних інструментів можна автоматично відстежувати хештеги, що використовуються для позначення подій, пов'язаних з війною, наприклад, #UkraineWar, #RussianAggression тощо;

аналіз медіаконтенту: використання інструментів, таких як InVID або Amnesty's YouTube Data API, для перевірки достовірності відео, що публікуються в мережі, з метою боротьби з дезінформацією та маніпуляціями;

аналіз геолокації: за допомогою метаданих, що супроводжують фотографії та відео (EXIF), можна точно визначити місце зйомки і порівняти з іншими джерелами інформації. Соціальні мережі дозволяють не тільки отримувати перші свідчення та підтвердження

подій, але й сприяють виявленню розвідки та інформаційних атак супротивника.

Інструменти для виявлення дезінформації та фактчекінгу. У воєнний час важливо не тільки отримувати інформацію, а й перевіряти її достовірність. Оскільки інформаційна війна є важливим елементом конфліктів, то поширення фейків і маніпуляцій може серйозно вплинути на ситуацію. Для боротьби з дезінформацією розроблено низку інструментів, які допомагають перевіряти факти:

TruthNest: інструмент для аналізу соціальних мереж, що дозволяє визначити, чи є певні пости та новини частиною інформаційної кампанії.

ClaimReview: платформа для автоматичної перевірки фактів і пошуку джерел, що підтверджують або спростовують новини.

FactCheck.org: ресурс, що спеціалізується на перевірці достовірності новин і документів.

Такі інструменти допомагають розпізнати фейкові новини, маніпуляції в соціальних мережах і коректно оцінити ситуацію на основі перевірених даних.

Інструменти збору та аналізу відкритих даних. Крім соціальних мереж та супутникових знімків, важливим інструментом OSINT є системи для збору та аналізу відкритих даних з публічних реєстрів, блогів, новинних сайтів, форумів, спеціалізованих порталів і навіть державних звітів. Інструменти для аналізу відкритих даних дозволяють автоматично агрегувати інформацію з різних джерел та проводити її систематичний аналіз для виявлення загроз або корисної інформації. До таких інструментів належать[17]:

Maltego[18]: потужний інструмент для візуалізації мережі зв'язків і аналізу даних, що дозволяє відстежувати зв'язки між різними суб'єктами та відстежувати їх діяльність в Інтернеті.

---

[17] Що таке OSINT (Open Source Intelligence, розвідка на основі відкритих джерел)? (2023). URL: https://thetransmitted.com/adlucem/shho-take-osint-open-source-intelligence-rozvidka-na-osnovi-vidkrytyh-dzherel/?utm_source=chatgpt.com

[18] Maltego. URL: https://www.maltego.com/

Shodan[19]: пошукова система, що дозволяє знаходити підключені до Інтернету пристрої та виявляти вразливості в інфраструктурі.

OSINT Framework[20]: набір інструментів і ресурсів для збору відкритих даних з різних джерел, від картографічних сервісів до інтернет-форумів.

Завдяки таким інструментам можна не тільки аналізувати поточну ситуацію, а й прогнозувати ймовірні розвитку подій, зокрема у військових діях.

Інструменти для моніторингу новин та автоматизованого збору даних. Системи моніторингу новин і автоматизованого збору даних дозволяють швидко реагувати на нові події. До таких систем належать:

NewsNow: агрегатор новин, який дозволяє відслідковувати новини за певними темами та ключовими словами.

Google Alerts: інструмент для налаштування сповіщень про нові публікації за конкретними словами або фразами.

Ці інструменти допомагають забезпечити моніторинг у реальному часі й оперативно реагувати на нові виклики.

Інструменти для аудіовізуального аналізу. Маніпуляції зі звуком та зображеннями — поширена техніка дезінформації. Військові використовують спеціалізовані інструменти для аналізу аудіо- та відеофайлів. Одним із таких інструментів є Deepware Scanner, який дозволяє виявляти маніпуляції з відео та аудіо даними, такі як фальсифікація звуків або зображень, що важливо в умовах дезінформаційних атак.

Використання технологічних інструментів OSINT під час воєнного стану є важливим елементом забезпечення національної безпеки та ефективного реагування на загрози. Завдяки супутниковим знімкам, соціальним мережам, інструментам для виявлення дезінформації та аналізу відкритих даних можна отримати

[19] Shodan. URL: https://www.shodan.io/

[20] OSINT Framework. URL: https://osintframework.com/?utm_source=chatgpt.com

важливу інформацію, що допомагає у плануванні операцій, моніторингу ситуації та прийнятті стратегічних рішень. Водночас важливою є боротьба з дезінформацією та захист від маніпуляцій, що є невід'ємною частиною сучасних військових конфліктів.

Загалом, у воєнний час OSINT виступає не лише інструментом оборони, а й фактором стримування противника: усвідомлення постійного моніторингу з відкритих джерел змушує сторони обмежувати свої дії, змінювати тактику, уникати компрометуючих ситуацій. На прикладі війни в Україні OSINT став ключовим джерелом для десятків структур — від міжнародних журналістів до українських військових підрозділів[21]. Так, відомими стали кейси використання TikTok-відео для виявлення переміщення техніки, фотографій із соціальних мереж для ідентифікації особового складу, супутникових фото для оцінки наслідків атак, зібраної аналітики у форматі геоінформаційних платформ. Аналітики, зокрема з Bellingcat, розробили методики дослідження таких відео, включаючи геолокацію та аналіз метаданих[22]. Прикладом, супутникових знімків, які використовуються для аналізу наслідків атак, можуть бути опубліковані знімки, що показували знищення російських гелікоптерів, після удару по аеродрому в Бердянську. Водночас такі ресурси як DeepStateMap, Liveuamap, GeoConfirmed стали щоденним інструментом мільйонів користувачів. Ці геоінформаційні платформи надають інтерактивні карти з інформацією про військові дії, переміщення техніки та наслідки атак.[23]

---

[21] Kalenský, J. & Osadchuk, R. (2024). Hybrid CoE: How Ukraine fights Russian disinformation: Beehive vs Mammoth.

[22] O'Connor, Ciarán (2022). How to Investigate TikTok Like a Pro — Part II: Using TikTok for Ukraine Research. URL: https://www.bellingcat.com/resources/how-tos/2022/11/02/how-to-investigate-tiktok-using-tiktok-ukraine-research/?utm_source=chatgpt.com

[23] Wikipedia: DeepStateMap.Live. URL: https://en.wikipedia.org/wiki/DeepStateMap.Live;

GeoConfirmed: Crowdsourced Geolocation OSINT Platform. URL: https://geoconfirmed.org

Ці приклади демонструють також, як OSINT став невід'ємною частиною сучасної розвідки та безпеки, особливо в умовах гібридної війни.

Однак ефективність OSINT визначається не лише кількістю зібраної інформації, а якістю її аналізу. Це вимагає фахової підготовки, розуміння контексту, уміння відрізняти маніпулятивні дані від достовірних, а також навичок командної роботи та використання спеціалізованих програм таких як Maltego, Palantir, Dataminr, Echosec, Sentinel Hub, Google Earth Pro, OSINT Combine та інші.[24]

Крім технологічного аспекту, важливо також розуміти соціальну динаміку OSINT. Війна цифрового покоління породжує нову культуру — культуру цифрових свідків, коли кожна публікація, зображення чи відео стає свідченням, доказом або орієнтиром. Це створює потужний інструмент мобілізації суспільства, але також і серйозну загрозу при відсутності контролю й аналізу наслідків.

Ризики, пов'язані з OSINT та інформаційною безпекою, в умовах воєнного стану

Аналіз та обробка відкритої інформації в умовах воєнного стану мають не лише очевидні переваги, а й пов'язані з численними ризиками, що можуть мати суттєвий вплив на національну безпеку та ефективність військових операцій. У контексті війни в Україні застосування методів OSINT продемонструвало як великий потенціал для стратегічного аналізу, так і серйозні небезпеки, зокрема щодо витоків чутливої інформації, маніпуляцій, кіберзагроз і фальсифікації даних. Розгляд цих аспектів є необхідним для розуміння як потенційних переваг, так і загроз використання відкритих джерел в умовах сучасного збройного конфлікту.

Ризики, пов'язані з використанням відкритих джерел, можуть мати різний характер і стосуватися не тільки державних

[24] Sentinel Hub. URL: https://www.sentinel-hub.com;
OSINT Combine — Professional OSINT Tools & Training. URL: https://www.osintcombine.com

структур, а й цивільних осіб, ЗМІ та інших учасників інформаційного середовища.

Зокрема, під час війни в Україні OSINT став важливим інструментом для військових, розвідки, а також для громадянського суспільства, що активно бере участь у боротьбі з агресором. Одним із найбільш яскравих прикладів використання OSINT в Україні є застосування відкритих джерел для виявлення позицій російських військ і військової техніки. Відкриті джерела, такі як супутникові знімки, соціальні мережі, відео з камер спостереження, публікації в блогах та онлайн-платформах, стали ключовими у зборі інформації.

Так, протягом війни українські волонтери та експерти використовували супутникові знімки для виявлення переміщення військової техніки та постачання, а також для аналізу змін на військових базах або складських приміщеннях супротивника. Наприклад, після масованих ударів російських військ по українських містах були проаналізовані знімки для підтвердження наявності російських установок та баз, що дозволило Збройним Силам України націлити контрзаходи, такі як удари по складах і мобільних ракетних системах.

Збір даних з відкритих джерел також дозволяє виявляти російських шпіонів та агентів, які намагаються проникнути в Україну. Наприклад, аналізуючи публікації, відео та фотографії, що з'являються на соціальних платформах, можна виявити осіб, які займаються шпигунською діяльністю або підготовкою до диверсій. Відкриті джерела стають важливим інструментом для встановлення контактів між російськими агентами та їхніми українськими спільниками.

Війна в Україні супроводжується активною інформаційною боротьбою та роз'яснювальною роботою, де OSINT використовується для розповсюдження правдивої інформації серед населення і для протидії російській пропаганді. Платформи, як Twitter, Telegram та інші соціальні мережі, стали майданчиками для розповсюдження фактів про бойові дії, ситуацію на фронті, гуманітарні питання, а також для контрпропаганди. Інформаційні

кампанії, що базуються на відкритих джерелах, допомагають посилити моральний дух населення, збільшити підтримку міжнародної спільноти та мобілізувати додаткові ресурси.

Численні переваги, використання OSINT супроводжуються певними ризиками і викликами, які потребують спеціального аналізу з погляду інформаційної безпеки. Так, в умовах воєнного стану в контексті використання OSINT особливо актуальними є такі загрози інформаційній безпеці як[25]:

ненавмисне розкриття критичної інформації (опубліковані фото чи відео з геолокацією, описами місця події, інформацією про пересування чи дислокацію підрозділів можуть використовуватися противником для нанесення ударів або проведення операцій впливу);

маскування дезінформації під OSINT (сторони конфлікту можуть цілеспрямовано поширювати фейки або перекручені факти у вигляді нібито відкритої інформації, які створюють викривлену картину подій, деморалізує населення, провокує паніку або підриває довіру до офіційних джерел);

автоматизоване використання OSINT-інструментів ворожими структурами (використання ботів, алгоритмів машинного навчання, інструментів збору великих масивів відкритих даних дозволяє ворогу отримувати стратегічну інформацію з відкритих українських ресурсів, соцмереж, реєстрів тощо);

підвищене навантаження на структури інформаційної безпеки (великий обсяг відкритих даних вимагає постійного моніторингу та оцінки ризиків. Органи, які забезпечують інформаційну безпеку, змушені працювати в режимі 24/7, реагуючи на нові загрози, фіксуючи витоки, розслідуючи інциденти);

порушення прав людини (у деяких випадках неконтрольоване використання відкритих даних для OSINT може призводити

[25] *Національна безпека: загрози та виклики* : матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 1 квітня — 12 травня 2024 року. Львів–Торунь : Liha-Pres, 2024. 256 с.

до втручання в приватне життя, розголошення персональних даних або публічного паплюження підозрюваних без належних доказів).

Інформаційна безпека в умовах воєнного стану може бути серйозно підкріплена або, навпаки, вразлива через кіберзагрози, що виникають внаслідок використання відкритих джерел[26]. Відкриті джерела можуть бути використані для проведення фішингових атак. Наприклад, використовуючи соціальні мережі, зловмисники можуть розміщувати фальшиві оголошення, що привертають увагу військових або громадян до фальшивих сторінок, які виглядають як офіційні ресурси уряду чи організацій. Такі сайти можуть бути використані для збору особистих даних, установлення шкідливого програмного забезпечення чи навіть організації атак на інші державні чи приватні ресурси. Кіберзлочинці можуть використовувати відкриті джерела для пошуку вразливостей у комп'ютерних системах, які взаємодіють із публічно доступною інформацією. У воєнний час важливіші таємниці і критична інфраструктура стають мішенню для атак, що можуть бути здійснені через отриману з відкритих джерел інформацію.

У процесі збору даних з відкритих джерел може виникнути проблема витоку чутливої інформації. Це може стосуватися не тільки даних про місцезнаходження військових об'єктів, а й особистої інформації, яка може бути використана для атак на цивільних осіб або військових[27]. Наприклад, активне використання геолокаційних даних у публікаціях та знімках, розміщених у соціальних мережах, може призвести до витоку важливої інформації про місцезнаходження захисників або об'єктів критичної інфраструктури. Ця інформація може бути використана противником для планування атак чи диверсій.

---

[26] Lieutenant, By and Romanow, Nicholas (2025). The Transparency Trap: Risks of Deception in the Age of OSINT. USNI Proceedings. URL: https://www.usni.org/magazines/proceedings/2025/january/transparency-trap-risks-deception-age-osint

[27] Amid War in Ukraine, Open-Source Intelligence Investigators Need Better Ethics. Scientific American. URL: https://www.scientificamerican.com/article/amid-war-in-ukraine-open-source-intelligence-investigators-need-better-ethics/

Одним з важливих етапів захисту критичної інформації є визначення її вразливих точок. З огляду на широке використання відкритих джерел, критичні дані можуть потрапляти у відкритий доступ з різних джерел. Це можуть бути[28]:

– *соціальні мережі та онлайн-платформи*. Особисті дані, фотографії, геолокаційна інформація можуть бути доступні через пости, відео та інші публікації. Протягом війни, наприклад, навіть невеликі помилки у публікаціях можуть призвести до розголошення важливої інформації;

– *супутникові знімки та геолокаційні дані*. Відкриті платформи супутникових знімків дозволяють отримати детальну інформацію про розташування об'єктів, переміщення військових сил та техніки;

– *інтернет-форуми, блоги та інші відкриті джерела*. Спільноти в Інтернеті, зокрема на платформах типу Reddit, можуть обговорювати важливі питання, надаючи велику кількість інформації, що містить фрагменти критичних даних;

– *публічні реєстри та бази даних*. Наприклад, публічні документи, які містять інформацію про організації, фінансові звіти, дані про осіб, можуть бути використані зловмисниками для маніпуляцій або інших незаконних дій.

Водночас захист критичної інформації в умовах доступності відкритих даних потребує запровадження технічних засобів і протоколів. До основних методів належать:

Шифрування даних. Одним із основних способів захисту критичної інформації є шифрування, яке забезпечує надійний захист даних від несанкціонованого доступу, навіть якщо ці дані потрапляють в Інтернет або зловмисники отримують до них доступ. Сучасні алгоритми шифрування дозволяють захистити як дані, що зберігаються на сервері, так і дані, що передаються по мережах зв'язку.

Захист від витоків даних (Data Loss Prevention, DLP). Системи захисту від витоків даних дозволяють контролювати та запобігати

[28] Their Photos Were Posted Online. Then They Were Bombed. URL: https://www.wired.com/story/wagner-group-osint-russia-ukraine/?utm_source=chatgpt.com

несанкціонованому розповсюдженню чутливих даних. Вони можуть виявляти спроби передачі важливої інформації через електронну пошту, веб-сайти або навіть через соціальні мережі.

Використання багатофакторної аутентифікації. Застосування багатофакторної аутентифікації є ще одним заходом для забезпечення безпеки даних, адже цей метод робить процес доступу до важливої інформації значно більш складним для зловмисників. Крім традиційних паролів, додаткові фактори аутентифікації (наприклад, відбитки пальців, смарт-карти, одноразові коди) значно підвищують рівень захисту.

Моніторинг та виявлення аномалій. Інтеграція систем моніторингу та виявлення аномалій дозволяє оперативно виявляти несанкціоновані спроби доступу до даних або їх викрадення. Ці системи здійснюють моніторинг всіх дій з інформацією, що зберігається в організації, і формують попередження про можливі загрози.

Невід'ємною частиною захисту критичної інформації є організаційні заходи. До них відносяться[29]:

Навчання та підвищення обізнаності. Захист критичної інформації значною мірою залежить від рівня обізнаності співробітників організації. Регулярне навчання та проведення тренінгів з питань безпеки дозволяє знизити ризики людських помилок, зокрема вразливості до фішингових атак, ненавмисного витоку інформації або неправильного поводження з чутливими даними.

Розробка політик безпеки. Розробка та впровадження політик безпеки, які чітко визначають правила обробки, зберігання та передавання критичних даних, є важливим етапом захисту. Це включає створення спеціальних процедур для роботи з конфіденційною інформацією, обмеження доступу до певних даних за посадами та необхідністю.

[29] Публічна інформація у формі відкритих даних в умовах воєнного стану: специфіка, парадокси, поради. URL: https://dostup.org.ua/blogs/publications/publichna-informatsiia-u-formi-vidkrytykh-danykh-v-umovakh-voiennoho-stanu-spetsyfika-paradoksy-porady?utm_source=chatgpt.com

Обмеження доступу до інформації. Необхідно впроваджувати принцип мінімальних прав доступу (Least Privilege), що означає, що кожен співробітник має доступ лише до тих даних, які йому необхідні для виконання своїх службових обов'язків. Це допомагає мінімізувати ймовірність витоку інформації через недобросовісних працівників або зовнішніх зловмисників.

Правові та етичні аспекти. Не менш важливим є правовий та етичний аспекти захисту інформації. Законодавство має надавати чіткі інструкції щодо того, які дані підлягають захисту, а які можна відкрито використовувати. Крім того, важливо забезпечити етичне використання відкритих даних, аби не порушувати права громадян на конфіденційність та не допустити маніпуляцій з інформацією.[30]

Захист критичної інформації в умовах широкої доступності відкритих даних вимагає комплексного підходу, що включає технічні, організаційні та правові заходи. Підвищення обізнаності громадян і працівників організацій, ефективне використання засобів шифрування, моніторинг та управління доступом до даних дозволяють забезпечити надійний захист в умовах сучасних загроз. Водночас захист інформації має бути збалансованим і не перешкоджати розвитку технологій, які спрощують доступ до даних, але водночас несуть ризики для національної безпеки та особистої приватності.

В умовах воєнного стану використання дезінформації та маніпуляцій стає одним з основних інструментів війни. Зокрема, різноманітні повідомлення в соціальних мережах, відео та фотографії, які з'являються в результаті діяльності військових і цивільних осіб, стали потужним інструментом для збору даних[31]. Наприклад, коли військовослужбовці російської армії розміщували в своїх

[30] Bolen, Scott (2024). The Ethical Considerations of OSINT: Privacy vs. Information Gathering. Medium. URL: https://medium.com/@scottbolen/the-ethical-considerations-of-osint-privacy-vs-information-gathering-63b5b2f76c55

[31] How to use open source intelligence data to debunk Russian disinformation. URL: https://ijnet.org/en/story/how-use-open-source-intelligence-data-debunk-russian-disinformation

соцмережах фотографії з місць дислокації, аналітики могли отримати точні координати для подальшого аналізу. Водночас відкриті джерела, зокрема соціальні мережі, можуть бути використані для поширення недостовірної чи маніпулятивної інформації, що може викликати паніку серед населення або сплутати ворога[32].

Разом з тим, дезінформація є однією з основних загроз. Російські пропагандисти активно використовують відкриті джерела для розповсюдження фальшивих новин, створення фейкових відео та фотографій, а також для поширення маніпуляцій, що можуть впливати на громадську думку[33]. Наприклад, під час активних боїв на сході України, російські медіа маніпулювали інформацією, використовуючи відео з відкритих джерел, та дискредитуючи українську армію на міжнародній арені. Це може призвести до ескалації конфлікту та загострення гуманітарної ситуації. Зловмисники можуть використовувати відкриті джерела для маніпуляцій із фактами, створюючи і поширюючи фальшиві новини. Такі новини можуть бути пов'язані з подіями на фронті, діяльністю військових сил чи навіть із псевдопідтвердженням важливих стратегічних рішень урядів. Це може призвести до помилкових стратегічних рішень, затримок у прийнятті важливих рішень або навіть до моральної деморалізації військових та цивільних осіб. Користувачі, які свідомо або несвідомо поширюють дезінформацію, можуть стати частиною інформаційної війни. Пропаганда, що використовує відкриті джерела, може маніпулювати думкою громадян, сприяти мобілізації чи деморалізації та підривати довіру до уряду чи інших важливих інституцій.

Окрім кіберзагроз, існують й фізичні ризики, які можуть виникати через розголошення інформації з відкритих джерел, зокрема вони можуть бути використані й для планування атак на критичні

[32] Amid War in Ukraine, Open-Source Intelligence Investigators Need Better Ethics. Scientific American. URL: https://www.scientificamerican.com/article/amid-war-in-ukraine-open-source-intelligence-investigators-need-better-ethics/

[33] The Role of OSINT in the Russia-Ukraine Conflict. Flashpoint. URL: https://www.flashpoint.io/resources/report/role-of-osint-russia-invasion-of-ukraine

інфраструктурні об'єкти[34]. Наприклад, супутникові знімки можуть допомогти визначити місця скупчення військових сил, об'єктів постачання або важливих військових установ. Ця інформація може бути використана ворогом для точних ударів, що призведе до руйнувань і втрат серед цивільного населення. Відкриті джерела можуть містити інформацію про транспортні маршрути, переміщення військових сил, логістичні дані, які можуть бути використані для фізичних атак. Інформація з відкритих джерел може бути використана для здійснення стратегічних ударів або саботажу.

Використання відкритих джерел може призвести до серйозних загроз для безпеки цивільних осіб. В умовах воєнного стану дані про переміщення біженців, волонтерів, постраждалих від бойових дій можуть стати доступними в результаті аналізу відкритих джерел[35]. Це може привести до витоків персональних даних і спричинити ризик фізичних нападів або інших форм насильства. Використання відкритих джерел може призвести до зниження анонімності цивільних осіб в Інтернеті. Ідентифікація особи через її діяльність в соціальних мережах чи в інших відкритих каналах може стати причиною переслідувань або стати об'єктом атак.

Для забезпечення ефективного регулювання та контролю обігу чутливої відкритої інформації держава повинна здійснити кілька ключових кроків[36]:

По-перше — створення чіткої правової бази для регулювання інформації. Одним із перших кроків має бути розробка

---

[34] Brandstaetter, Sigmund (2024). The Dark Side of Open Source Intelligence: How Attackers Weaponize OSINT for Reconnaissance and Targeted Attacks. Medium. URL: https://osintph.medium.com/the-dark-side-of-open-source-intelligence-how-attackers-weaponize-osint-for-reconnaissance-and-43fb889ccc2a

[35] Karalis, Magdalene (2022). Open-source intelligence in Ukraine: Asset or liability? Chatham House. URL: https://www.chathamhouse.org/2022/12/open-source-intelligence-ukraine-asset-or-liability

[36] Бем М., Городиський І. (2021). Захист персональних даних: правове регулювання та практичні аспекти : науково-практичний посібник. URL: https://ombudsman.gov.ua/storage/app/media/uploaded-files/Handbook_Pers_Data_Protect_2021.pdf?utm_source=chatgpt.com

та вдосконалення правової бази, яка забезпечує чітке визначення, яка інформація є чутливою і яка потребує обмеження доступу. Це може включати законодавчі акти, що регулюють: *класифікацію чутливої інформації* (необхідно чітко визначити, що саме вважається чутливою інформацією, зокрема щодо національної безпеки, економічних питань, військових операцій, а також конфіденційних даних про громадян); *механізми обмеження доступу* (встановлення обмежень на доступ до інформації, яка може завдати шкоди, особливо в умовах війни, наприклад, за допомогою національних стандартів захисту інформації (таких як ISO/IEC 27001)[37]); *принципи доступу та обміну інформацією* (визначення чітких процедур для обміну чутливою інформацією між державними органами, приватними компаніями, а також міжнародними партнерами). Це також включає розробку процедур для своєчасного оновлення статусу інформації в залежності від зміни обставин, таких як закінчення воєнного стану чи зміна військової ситуації.

По-*друге — забезпечення ефективного контролю за обігом чутливої інформації в Інтернеті*. Одним із найскладніших аспектів є контроль за інформацією в Інтернеті, де обсяг даних неймовірно великий, а доступ до них — майже миттєвий. Держава має:

співпрацювати з інтернет-компаніями: уряди повинні налагоджувати співпрацю з інтернет-платформами, такими як Google, Facebook, Twitter, YouTube, для швидкого виявлення і блокування чутливої інформації, що може загрожувати безпеці держави. Це включає механізми виявлення і видалення матеріалів, що містять стратегічно важливу інформацію, наприклад, розташування військових об'єктів або подробиці операцій;

заборонятиˌ публікації з певними даними: у випадках, коли інформація може бути використана для порушення безпеки

[37] Нова версія стандарту ISO/IEC 27001:2022: чим IT-компаніям корисний цей стандарт та як його впровадити. URL: https://ain.ua/2022/12/06/nova-versiya-standartu-iso-iec-270012022-chym-it-kompaniyam-korysnyj-czej-standart-ta-yak-jogo-vprovadyty/?utm_source=chatgpt.com

або для підготовки терористичних атак, держава може вводити заборони на публікацію таких даних, передбачаючи юридичні наслідки для порушників;

моніторити та виявляти маніпуляції: важливо забезпечити наявність систем для моніторингу в Інтернеті на предмет публікацій чутливої інформації, використовуючи як автоматизовані системи (наприклад, спеціальні алгоритми для виявлення небезпечних даних), так і участь спеціалізованих агентств (зокрема, кіберполіції).

По-третє — формування системи захисту критичної інфраструктури та даних. Ще одним важливим напрямком є захист інформації, що стосується критичної інфраструктури, зокрема енергетичних об'єктів, транспортних систем, військових баз і баз даних. Держава має вжити відпорні заходи щодо:

системи кібербезпеки та захисту інформаційних систем: захист критичних інформаційних систем від кібератак є основою державної безпеки. Для цього повинні бути створені спеціалізовані кіберпідрозділи, які забезпечують постійний моніторинг та захист від хакерських атак;

шифрування та захисту комунікацій: всі засоби комунікації, що використовуються для обміну чутливою інформацією між державними органами, повинні мати високий рівень захисту — шифрування, багаторівнева аутентифікація тощо;

інструментів для захисту даних у реальному часі: для мінімізації ризиків витоку чутливої інформації в реальному часі повинні застосовуватися технології, які дозволяють аналізувати потоки даних, виявляти потенційні загрози та запобігати їх поширенню.

По-четверте — освітні та інформаційні кампанії щодо безпеки інформації. Держава також повинна активно впроваджувати інформаційні кампанії для підвищення обізнаності населення про загрози, пов'язані з неконтрольованим обігом чутливої інформації. Це включає *освітні програми для громадян* (програми навчання, які пояснюють, які дані є чутливими, як їх захищати і чому важливо дотримуватися обмежень на публікацію певних видів інформації)

та *програми для державних службовців* (спеціалізовані тренінги для державних службовців і представників силових структур щодо ефективного використання і захисту чутливої інформації, а також розпізнавання можливих загроз на рівні особистої безпеки).

По-п'яте — міжнародна співпраця з іншими державами та організаціями. У світі глобалізації інформації жодна країна не може діяти ізольовано, тому важливо укладати міжнародні угоди та співпрацювати з іншими державами та міжнародними організаціями для обміну інформацією та взаємної підтримки у боротьбі з загрозами, що виникають через відкриті джерела.

Кроки можуть включати *укладання угоди з міжнародними організаціями* (наприклад, з Інтерполом, Європолом, ООН для обміну інформацією та співпраці в сфері кібербезпеки) та *спільні тренування й навчання* (проведення спільних заходів з іншими країнами щодо виявлення і протидії витоку чутливої інформації).

По-шосте — розвиток технологій для обмеження доступу до чутливої інформації. З розвитком технологій виникають нові методи для захисту чутливої інформації. Сучасні технології дозволяють *розробляти алгоритми для автоматичного виявлення чутливої інформації* (створення спеціалізованих інструментів для автоматичного аналізу великих масивів даних з метою виявлення і класифікації чутливої інформації) та *блокувати певні джерела або типи даних* (використання технологій блокування даних за ключовими словами або шаблонами, що дозволяє швидко зупиняти поширення небезпечної інформації).

Регулювання обігу чутливої відкритої інформації є складним і багатогранним процесом, що вимагає комплексного підходу, включаючи розробку правових норм, створення механізмів для контролю за інформаційними потоками, забезпечення захисту критичної інфраструктури та активне співробітництво з міжнародними партнерами. Держава повинна адаптувати свої стратегії та засоби захисту до нових реалій інформаційної війни, враховуючи як технологічні, так і етичні аспекти.

Правові та етичні аспекти використання OSINT

Ще одним важливим аспектом є етичний вимір використання OSINT. В умовах воєнного часу органи влади, приватні особи і навіть медіа можуть використовувати дані з відкритих джерел, що підпадають під певні етичні й правові обмеження. Інколи інформація, що потрапляє до відкритого доступу, може порушувати права людини на конфіденційність або стати підставою для незаконних репресій.

Хоча інформація, яка використовується у межах OSINT, формально є відкритою, її добування, аналіз та подальше використання має відповідати як національному законодавству, так і міжнародним правовим стандартам. Порушення меж дозволеного може призводити до втручання в приватне життя, неправомірного стеження або навіть розкриття чутливої інформації, яка може нашкодити як особам, так і державним інтересам. Особливо під час воєнного стану необхідно уникати шкоди цивільним особам при зборі та поширенні відкритої інформації[38]. Для спільноти OSINT важливим має бути приділення більшої уваги етичним питанням, таким як ризики для цивільного населення та можливе використання інформації ворогом, а також у роботі з відкритими джерелами ключовим має бути принцип «не нашкодь».[39]

З юридичного погляду, в українському законодавстві відсутнє чітке визначення OSINT як інструменту розвідки або правоохоронної діяльності. Водночас Закон України «Про розвідку» (ст. 10)[40] допускає використання відкритої інформації у межах

[38] Millett, Ed (2023). Deploying OSINT in Armed Conflict Settings: Law, Ethics, and the Theory of Harm. ICRC: International Committee of the Red Cross. URL: https://blogs.icrc.org/law-and-policy/2023/12/05/deploying-osint-in-armed-conflict-settings-law-ethics-theory-of-harm/

[39] Amid War in Ukraine, Open-Source Intelligence Investigators Need Better Ethics. Scientific American. URL: https://www.scientificamerican.com/article/amid-war-in-ukraine-open-source-intelligence-investigators-need-better-ethics/

[40] Про розвідку : Закон України від 17 вересня 2020 року № 912-IX. URL: https://zakon.rada.gov.ua/laws/show/912-20#n36

розвідувальної діяльності. КПК України дозволяє використання відкритих джерел для збирання відомостей, однак не надає прямої вказівки на їх допустимість як доказів у суді. Це створює правову невизначеність та потенційно ускладнює легітимність дій правоохоронних і розвідувальних органів, які застосовують OSINT у межах своєї діяльності.

Особливо чутливими є ситуації, коли OSINT застосовується до приватних осіб, журналістів або учасників мирних ініціатив. В умовах війни межа між національною безпекою та свободою слова/правом на приватність значно звужується, що створює ризики зловживань. Досвід використання відкритих джерел у конфліктах, таких як війна в Україні та в Сирії, підкреслює необхідність розробки стандартів для їх правового використання[41]. Тому впровадження етичних стандартів і внутрішніх протоколів має стати обов'язковою практикою для організацій, які використовують відкриту розвідку.

Етичні виклики OSINT охоплюють баланс між прозорістю та безпекою (надмірне поширення навіть відкритої інформації може сприяти ворогу в плануванні атак); ідентифікацію джерел (добування інформації з напівзакритих спільнот, форумів або соціальних мереж може містити ознаки соціальної інженерії або маніпуляцій); право на забуття (навіть відкриті цифрові сліди мають зберігати контекст і терміни актуальності; використання застарілих або вирваних із контексту даних може завдати шкоди особі); добровільність (участь волонтерів і громадян у OSINT-проєктах має бути усвідомленою та із чітким розумінням ризиків).

Забезпечення належного балансу між відкритістю інформації та національною безпекою в умовах воєнного стану є складним завданням. Природа цього балансу полягає у визначенні

[41] Dirisu, Deniz Mykola and Balbinot, Manon-Catherine (2025). Institutionalization: A Way Forward to Prove the Role of Open-Source Intelligence to the Courts. URL: https://opiniojuris.org/2025/04/28/institutionalization-a-way-forward-to-prove-the-role-of-open-source-intelligence-to-the-courts/

меж між доступністю важливих даних для громадян та захистом критично важливої інформації, яка може бути використана для завдання шкоди державним інтересам[42]. У цьому контексті необхідно враховувати як державні інтереси безпеки, так і права та свободи громадян, а також етичні стандарти в роботі з відкритими джерелами.

Перш за все, важливо зазначити, що не вся інформація, що знаходиться в публічному доступі, може бути безпечною для широкого використання. У воєнний час особливу увагу слід звернути на такі види інформації:

1. *Військова інформація*. Інформація, яка стосується розташування військових частин, стратегічних об'єктів, руху військової техніки, а також плани та операції, що можуть бути використані противником для здійснення атак. Такі дані повинні бути обмеженими, й їхній доступ необхідно регулювати, щоб уникнути випадкових або навмисних витоків, які можуть зашкодити безпеці держави.

2. *Критична інфраструктура*. Інформація щодо роботи критичної інфраструктури, зокрема енергетичних об'єктів, водопостачання, транспорту, телекомунікацій, повинна бути обмежена, щоб не дати можливість противнику здійснити кібератаки або інші види саботажу.

3. *Інформація про військових і правоохоронців*. Збір даних про особовий склад армії, сил безпеки та правоохоронних органів, а також їхню діяльність може становити загрозу для життя і безпеки осіб, які беруть участь у війні чи підтримують порядок. Розкриття такої інформації може призвести до персональних атак чи інших форм насильства.

4. *Інформація щодо національної оборонної стратегії та безпеки*. Дані, що стосуються стратегічних напрямків розвитку оборонної політики країни, вразливих точок у системі національної

[42] Libicki, M. C. (2007). Conquest in Cyberspace: National Security and Information Warfare. Cambridge University Press

безпеки, а також плани на випадок загострення ситуації, повинні залишатися конфіденційними.

5. *Особиста інформація громадян, зокрема, дані про біженців та переселенців*. У воєнний час захист приватності громадян стає критично важливим. Невірне використання даних про переселенців, учасників бойових дій або цивільних осіб може призвести до наслідків, що загрожують їхній безпеці, зокрема, якщо ці дані потраплять до ворога чи злочинців.

Для визначення меж публічності цієї інформації необхідно, щоб держава проводила ретельну класифікацію даних, регулярно оцінюючи їхній рівень чутливості та визначаючи, які з них можуть бути доступні для громадян, а які повинні бути обмежені. Рішення про обмеження доступу до інформації повинні ґрунтуватися на об'єктивних критеріях, таких як ступінь загрози національній безпеці, а також на принципах законності та етики.[43]

Важливою складовою забезпечення балансу між відкритістю та безпекою є саморегуляція різних органів у суспільстві, зокрема держави, громадських організацій, медіа та інших учасників[44]. Ця саморегуляція є необхідною для забезпечення ефективної та безпечної роботи з інформацією у відкритих джерелах, особливо в умовах воєнного стану.

Держава є головним регулятором інформаційних потоків і повинна забезпечити належні механізми захисту національної безпеки через законодавчі ініціативи, а також визначення чітких процедур і правил щодо доступу до відкритої інформації. У цьому контексті держава повинна *створювати нормативно-правову базу, яка визначатиме, які види інформації є конфіденційними і повинні бути обмежені; формувати органи, які відповідатимуть*

[43] United Nations Human Rights Council (2022). Right to Privacy in the Digital Age (A/HRC/51/17). URL: https://digitallibrary.un.org/record/3985679?v=pdf

[44] Open Source Intelligence: Risks, Challenges and Ethical Boundaries. NATO StratCom COE (2022). URL: file:///C:/Users/%D0%9D%D0%B0%D1%82%D0%B0%D0%BB%D0%B8%D1%8F/Downloads/Information-Conflict-DIGITAL-FINAL.pdf

за моніторинг і захист важливих інформаційних ресурсів, а також організовувати механізми відповідальності за порушення правил збору та обробки відкритої інформації.

В умовах воєнного стану громадські організації, волонтери та інші представники громадянського суспільства мають важливу роль у контролі за використанням відкритих джерел інформації. Вони можуть допомагати у виявленні несанкціонованих витоків інформації, брати участь у перевірці фактів і надавати зворотний зв'язок щодо того, що є безпечним для публікації, а що — може загрожувати безпеці. Водночас громадянське суспільство може ініціювати програми інформування громадян щодо важливості захисту своїх особистих даних і унеможливлення доступу до інформації, яка може бути використана для маніпуляцій чи шкоди.

Медіа у воєнний час мають особливу відповідальність щодо того, яку інформацію вони публікують. Журналісти повинні бути обізнаними щодо наслідків публікацій і здатними обирати, що є важливим для громадян, а що може створити ризики для безпеки. Важливо, щоб медіа не лише повідомляли про події, але й активно займалися фактчекінгом, перевіркою інформації та протидією дезінформації, яка може бути поширена як частина інформаційної війни. Крім того, медіа повинні бути відкритими для обговорення та саморегуляції, зокрема в питанні коректності подачі чутливої інформації.[45]

Законодавство в сфері управління інформацією повинно базуватися на низці основних принципів, зокрема:

Принцип захисту національної безпеки. Законодавчі акти повинні регламентувати, яку інформацію можна оприлюднювати без шкоди для безпеки держави. Це включає розробку нормативно-правових актів, що визначають межі відкритих джерел і регулюють їх використання в інтересах безпеки.

[45] ЗМІ і війна: Особливості поширення інформації та фото під час воєнного стану (2022). Платформа прав людини. URL: https://ppl.org.ua/zmi-i-vijna-osoblivosti-poshirennya-informaci%D1%97-ta-foto-pid-chas-voyennogo-stanu.html?utm_source=chatgpt.com

Принцип захисту прав людини. Права людини повинні бути пріоритетними і закони не повинні порушувати основні свободи громадян, зокрема право на приватність та свободу висловлювань. Водночас в умовах воєнного стану потрібно дотримуватися балансу між свободою інформації та необхідністю захисту безпеки.

Принцип прозорості та підзвітності. Всі державні дії, що стосуються збору та поширення інформації, повинні бути підзвітними громадянам. Це включає надання можливості громадськості перевіряти законність і етичність використання відкритих джерел.

Принцип саморегуляції. Важливим є створення організацій, які забезпечують саморегуляцію в медіа та громадських організаціях. Ці органи повинні визначати етичні норми для роботи з відкритими джерелами, щоб зменшити ризики зловживань.

Баланс між відкритістю та безпекою є критично важливим аспектом у використанні OSINT в умовах воєнного стану. Забезпечення належного рівня доступу до інформації, що не становить загрози національній безпеці, і одночасно захист важливої інформації від витоків є надзвичайно складною задачею, що вимагає активної участі держави, суспільства та медіа. Законодавчі та етичні норми повинні чітко визначати межі цього балансу, гарантувати захист прав людини та зберігати високий рівень безпеки для держави.

З огляду на це, необхідним є створення національної етичної рамки для використання OSINT, яка враховуватиме *вимоги до прозорості алгоритмів збору інформації, стандарти відповідального аналізу, принципи мінімізації шкоди, а також вимоги до захисту персональних даних навіть у публічному просторі*.

У воєнних умовах особливу роль відіграє також координація з військовими структурами щодо того, яка інформація є допустимою до поширення, а яка має обмежуватись у публічному обігу навіть попри її відкритий характер. Випадки публікації фото техніки, маршрутів або розташування військових частин через

соціальні мережі демонструють вразливість OSINT-практик без належного правового й етичного регулювання[46].

Правове та етичне забезпечення OSINT є критично важливим як для захисту національних інтересів, так і для збереження легітимності та довіри до державних інституцій і громадянських ініціатив. У цьому контексті важливим кроком має стати оновлення законодавства, розробка кодексів етики для відповідних фахівців, а також створення міжвідомчих протоколів використання відкритих джерел у межах безпекової діяльності.

Ці фактори зумовлюють необхідність поєднувати розвиток OSINT з належними інструментами захисту інформаційної сфери. Йдеться про законодавче регулювання, стандарти поведінки в мережі, технічні рішення з фільтрації критичної інформації, системи попередження про загрози, а також — інформаційно-просвітницьку роботу з населенням.

Розвиток культури відповідального користування відкритими джерелами є одним із ключових аспектів забезпечення інформаційної безпеки в умовах війни. Це має охоплювати не лише професіоналів, а й широкий загал — адже у цифровому середовищі кожен громадянин потенційно є і споживачем, і поширювачем, і джерелом інформації.

У цьому контексті важливо не протиставляти OSINT та інформаційну безпеку, а інтегрувати їх у спільну екосистему — де розвідка з відкритих джерел стає інструментом не лише збору даних, а й превенції, ідентифікації загроз, формування стійкості суспільства до маніпуляцій і атак.

Таким чином, ризики, пов'язані з використанням відкритих джерел під час воєнного стану, можуть бути багатогранними і серйозними. Вони охоплюють як можливі витоки чутливої інформації, так і можливість маніпуляцій через дезінформацію, кіберзагрози, фізичні атаки

[46] Open Source Intelligence: Risks, Challenges and Ethical Boundaries. NATO StratCom COE (2022). URL: file:///C:/Users/%D0%9D%D0%B0%D1%82%D0%B0%D0%BB%D0%B8%D1%8F/Downloads/Information-Conflict-DIGITAL-FINAL.pdf

на інфраструктуру та загрози для безпеки громадян. Для мінімізації цих ризиків необхідно розвивати систему безпеки в межах використання відкритих джерел, зокрема, зосередивши увагу на моніторингу інформаційного простору, ефективному використанні технологій для аналізу та перевірки фактів, а також постійно адаптуючи політику безпеки відповідно до змінюваних умов воєнного часу.

Розвиток інституційної спроможності щодо OSINT в Україні

Важливим є вивчення нагальних питань щодо інституційної спроможності України в царині OSINT та у сфері захисту інформаційного простору в умовах збройної агресії рф.

Розвиток інституційної спроможності в сфері OSINT та інформаційної безпеки в Україні є ключовим компонентом протистояння гібридній агресії, забезпечення сталості державного управління та адаптації до нових викликів інформаційного середовища. В умовах воєнного стану формування цілісної та ефективної інституційної архітектури у цій сфері стає не лише питанням ефективності державної політики, але й умовою збереження державності та суспільної цілісності.

Після 2014 року, а особливо з початку повномасштабної агресії рф у 2022 році, Україна докорінно переглянула підходи до функціонування сектору безпеки в інформаційному вимірі. Було створено або реформовано низку інституцій — ключові державні та недержавні суб'єкти, — що відіграють провідну роль у сфері OSINT, інформаційного моніторингу, кіберзахисту та протидії інформаційним операціям.

Так, зокрема, *Головне управління розвідки Міністерства оборони України (ГУР МО)* — провідний орган воєнної розвідки — активно використовує OSINT як доповнення до HUMINT, SIGINT, IMINT та інших джерел. Публічні звіти ГУР містять дані, що базуються на відкритих джерелах, зокрема при виявленні розташування ворожих підрозділів, фіксації воєнних злочинів та прогнозуванні дій противника.

Підрозділи *Служби безпеки України (СБУ)* здійснюють контррозвідку в цифровому середовищі, викривають шпигунську діяльність, координують роботу з виявлення інфраструктури ворожих бот-мереж та розслідують факти поширення дезінформації. У структурі СБУ діють підрозділи з кібербезпеки, які використовують OSINT для виявлення та документування діяльності колаборантів, агентури впливу, каналів інформаційних вкидів.

Ключовий правоохоронний орган — *Кіберполіція України* — спеціалізується на кіберзлочинах. OSINT для кіберполіції є джерелом доказової бази у справах, пов'язаних із фішингом, шахрайством, пропагандистськими ресурсами та інфраструктурою ворожих інформаційних впливів.

Органом, який відповідальний за технічний захист інформації, кіберзахист критичної інфраструктури, а також координацію взаємодії у сфері інформаційної безпеки між державними органами та приватним сектором, є *Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ)*. Через CERT-UA (національний центр реагування на комп'ютерні інциденти) відбувається обробка інцидентів, у тому числі на основі OSINT-джерел.

Міністерство цифрової трансформації України займається розвитком відкритих державних даних, діджиталізацією адміністративних процесів, а також підтримує реалізацію інформаційної політики, включаючи боротьбу з фейками, кібергігієну, медіаграмотність. Цей орган координує відкритість даних, які згодом використовуються OSINT-аналітиками.

Створений при Міністерстві культури та інформаційної політики України *Центр стратегічних комунікацій та інформаційної безпеки* виконує функції з аналізу інформаційного середовища, контрпропаганди, координації стратегічних наративів держави, а також взаємодії з міжнародними партнерами. Центр активно використовує аналітику OSINT у комунікаційній протидії російським ІПсО.

У даному контексті не можливо не зауважити на важливості ролі *громадянського суспільства та волонтерських ініціативах*.

Українська специфіка полягає у високій активності недержавних суб'єктів: волонтерських OSINT-спільнот, блогерів-розслідувачів, журналістів-розвідників. Такі ініціативи як InformNapalm, Molfar, DeepState, Bihus.Info, OSINT-UA, Data Journalism Agency (TEXTY) здійснюють ґрунтовні розслідування, зокрема щодо воєнних злочинів, переміщення техніки, ідентифікації військовослужбовців рф тощо. Вони доповнюють зусилля держави та є унікальною формою інформаційного спротиву.

Цей інституційний перелік організацій характеризується *поліцентричністю* (наявністю кількох ключових гравців із різною юрисдикцією), *горизонтальними зв'язками між державою і громадянським суспільством, високим рівнем імпровізації та адаптації до загроз, зростаючим рівнем професіоналізації аналітики з відкритих джерел*.

Водночас, не дивлячись на те, що з початку повномасштабної агресії рф інституційна спроможність України у сфері OSINT та інформаційної безпеки значно зросла, а скоординована діяльність державних органів та громадянського суспільства забезпечує більш ефективну протидію інформаційним загрозам та сприяє зміцненню національної безпеки, існують виклики.

По-перше, все ще залишається недостатня міжвідомча координація. Попри зусилля та наявні ініціативи Ради національної безпеки і оборони України, взаємодія між державними органами у сфері OSINT є недостатньо системною або не має чітко визначених процедур та у неповній мірі регламентована на інституційному рівні.

По-друге, відсутній єдиний централізований інституційний центр компетентності у сфері OSINT (або центр OSINT-компетентності). На сьогодні в Україні не існує єдиної централізованої державної структури, яка б відповідала за розробку уніфікованої методології, підготовку, навчання та сертифікацію фахівців з OSINT у публічному секторі. Така фрагментація унеможливлює формування цілісної системи знань і стандартів у цій галузі.

По-третє, все ще існує кадровий дефіцит у сфері OSINT-аналітики. Ринок аналітиків OSINT ще не сформувався повною мірою.

Відчутною є нестача кваліфікованих кадрів, які володіють сучасними інструментами OSINT, мають розвинене аналітичне мислення, знання цифрової криміналістики та навички роботи з великими масивами відкритих даних.

По-четверте. Недостатнє правове регулювання. На нормативно-правовому рівні відсутнє чітке правове визначення статусу OSINT-даних у контексті кримінального процесу. Крім того, не врегульовано процедури збору, зберігання, обробки та використання інформації з відкритих джерел у межах оперативно-розшукової та слідчої діяльності, що створює ризики правової невизначеності.

Використання OSINT в умовах воєнного стану вимагає тісної співпраці між державними і недержавними органами, адже питання національної безпеки, розвідки та інформаційної безпеки не можуть бути вирішені лише зусиллями державних органів[47]. Паралельно з офіційними структурами, важливу роль відіграють громадські організації, волонтери, незалежні журналісти та приватні компанії, які можуть надавати цінну інформацію для розв'язання стратегічних завдань, зокрема у контексті воєнних дій.

Державні органи, зокрема розвідувальні та правоохоронні служби, мають особливу відповідальність за збір, аналіз і використання OSINT для забезпечення національної безпеки. Вони використовують ці дані для стратегічних прогнозів, запобігання загрозам, а також для планування військових та інших безпекових операцій. В умовах воєнного стану, коли традиційні методи розвідки можуть бути обмежені або ускладнені, відкриті джерела інформації стають важливим інструментом для отримання швидких і точних відомостей про дії противника[48].

[47] NATO Strategic Communications Centre of Excellence. URL: https://stratcomcoe.org/publications?aid[]=22

[48] Bazzell, M. (2022). *Open source intelligence techniques: Resources for searching and analyzing online information* (10th ed.). Intel Techniques;

Artificial intelligence, big data and fundamental rights. European Union Agency for Fundamental Rights. URL: https://fra.europa.eu/en/project/2018/artificial-intelligence-big-data-and-fundamental-rights

Розвідувальні служби, як правило, мають доступ до спеціалізованих баз даних, технологій для збору даних з Інтернету, а також інструментів для їх аналізу. Вони повинні діяти в межах законодавства, забезпечуючи при цьому не лише національну безпеку, але й захист прав громадян[49]. Важливо зазначити, що будь-які дії державних органів щодо збору відкритої інформації повинні бути прозорими та підзвітними громадськості, аби уникнути порушень етичних і правових стандартів.

Незважаючи на важливість державних органів у забезпеченні національної безпеки, недержавні органи також можуть значно сприяти ефективності використання OSINT. Громадські організації, зокрема, часто здійснюють моніторинг та збір інформації щодо порушень прав людини, воєнних злочинів і атак на цивільне населення[50]. Вони можуть діяти на місцях, надаючи оперативні дані про ситуацію на фронті або в тилу, що особливо важливо в умовах швидко змінюваної обстановки.

Волонтери та неурядові організації також активно долучаються до збору даних з відкритих джерел, що стосуються гуманітарної ситуації, руху біженців або допомоги мирним жителям. Часто вони використовують соціальні мережі для моніторингу ситуації та виявлення нових загроз чи порушень, які можуть бути пропущені державними органами.

Серед недержавних органів варто відзначити і незалежних журналістів, які займаються фактчекінгом і верифікацією інформації, наданої в різних відкритих джерелах. Вони відіграють ключову роль у боротьбі з дезінформацією, особливо в умовах інформаційних

---

[49] Guidelines on the Protection of Human Rights Defenders. URL: https://www.osce.org/files/f/documents/c/1/119633.pdf

[50] Bellingcat. (n.d.). Bellingcat — the home of online investigations. URL: https://en.wikipedia.org/wiki/Bellingcat;

Conflict Observatory. (n.d.). Conflict Observatory. URL: https://en.wikipedia.org/wiki/Conflict_Observatory

воєн[51]. Журналісти, використовуючи доступні ресурси, можуть створювати незалежні та достовірні матеріали, що сприяють об'єктивному висвітленню ситуації в країні та за її межами.

Приватні компанії, зокрема ті, що працюють у сфері кібербезпеки, також можуть відігравати важливу роль у використанні OSINT. Вони здатні надати технологічну та аналітичну підтримку органам державної влади, надаючи їм інструменти для збору та обробки великих обсягів відкритої інформації.

Співпраця між державними та недержавними органами в сфері OSINT повинна ґрунтуватися на чітких принципах і нормах. Це дозволить уникнути потенційних ризиків, пов'язаних із зловживанням інформацією, а також забезпечити ефективне і етичне використання даних. Одним з ключових аспектів такої співпраці є обмін інформацією, де державні органи повинні надавати громадським організаціям та журналістам доступ до важливих даних, коли це не суперечить інтересам національної безпеки.[52]

Іншою важливою складовою є координація дій. У випадку надзвичайних ситуацій, таких як інформаційні атаки або кібератаки, державні органи і приватні компанії повинні мати механізми для оперативного реагування на загрози та нейтралізації їх наслідків. Також важливими є спільні тренінги та навчання з обробки даних, обміну досвідом та технологічними новинками в сфері OSINT.

Проте, для забезпечення ефективної співпраці важливо встановити чіткі межі дозволеного збору інформації, визначити критерії,

---

[51] The Power of OSINT in the Digital Age: Boosting fact-checking & investigative journalism (2023). Warsaw Institute. URL: https://warsawinstitute.org/the-power-of-osint-in-the-digital-age-boosting-fact-checking-investigative-joirnalism/?utm_source=chatgpt.com;

Bellingcat. (n.d.). Bellingcat — the home of online investigations. URL: https://en.wikipedia.org/wiki/Bellingcat;

Conflict Observatory. (n.d.). Conflict Observatory. URL: https://en.wikipedia.org/wiki/Conflict_Observatory

[52] Open Source Intelligence: Risks, Challenges and Ethical Boundaries. NATO StratCom COE. (2022). URL: file:///C:/Users/%D0%9D%D0%B0%D1%82%D0%B0%D0%BB%D0%B8%D1%8F/Downloads/Information-Conflict-DIGITAL-FINAL.pdf

за якими надаватиметься доступ до відкритих джерел, та механізми захисту від зловживань. Водночас необхідно забезпечити дотримання прав людини та етичних стандартів аби співпраця між державними і недержавними органами була конструктивною та безпечною для всіх учасників.

У майбутньому, з розвитком нових технологій і збільшенням обсягів доступної відкритої інформації, роль OSINT буде лише зростати. Співпраця між державними та недержавними органами стане ще більш важливою, оскільки нові загрози, зокрема кібератаки та дезінформація, потребуватимуть комплексного реагування та оперативного обміну даними.

Одним з важливих кроків у цьому напрямку є створення єдиних платформ для збору та аналізу даних, що дозволить забезпечити ефективний обмін інформацією між державними установами, приватними компаніями та громадськими організаціями. Крім того, важливою складовою стане розробка міжнародних стандартів для використання OSINT, що дозволить забезпечити єдність підходів до збору та обробки даних у межах глобальних загроз, зокрема інформаційних воєн.

Таким чином, взаємодія між державними та недержавними органами в сфері OSINT є важливою складовою забезпечення національної безпеки в умовах воєнного стану. Така співпраця дозволяє максимально ефективно використовувати відкриті джерела для отримання важливої інформації, водночас забезпечуючи баланс між безпекою та правами громадян.

Інституційна спроможність у сфері OSINT значною мірою залежить від взаємодії з міжнародними партнерами. Україна активно співпрацює із структурами НАТО, ЄС, ООН, а також із профільними організаціями, такими як EUROPOL, INTERPOL, European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), EU vs Disinfo, OCCRP та іншим.

Завдяки цій співпраці Україна отримує *доступ до міжнародних OSINT-платформ і баз даних, можливість стажування кадрів,*

технічну допомогу для створення OSINT-центрів, спільні розслідування з міжнародними командами, рекомендації щодо побудови інституційної екосистеми та протидії дезінформації.

Зокрема, в межах співпраці з EUAM Ukraine та StratCom CoE відбувається навчання офіцерів поліції та Збройних Сил України з методів OSINT, комунікаційного менеджменту та цифрової ідентифікації загроз[53].

Наявність спільних OSINT-проєктів (наприклад, міжнародні розслідування воєнних злочинів, документування геноциду, ідентифікація воєнних злочинців рф) підвищує глобальну довіру до українських розслідувачів та сприяє включенню національних інституцій у транснаціональні аналітичні мережі.

Разом із тим, постає потреба в інституціоналізації обміну даними на рівні державних структур, створенні єдиної національної системи OSINT-доступу до відкритих державних джерел, а також у формуванні національного OSINT-хабу, який міг би інтегрувати державні, академічні та громадянські ініціативи в єдину аналітичну систему.

Розвиток сектору національної безпеки та стійкості інформаційного простору в умовах гібридної агресії з боку російської федерації актуалізував потребу в якісно новому рівні аналітичної підтримки процесів прийняття рішень. Одним із ключових чинників забезпечення цієї спроможності є наявність підготовлених фахівців у сфері відкритої розвідки (OSINT), які здатні працювати в динамічному інформаційному середовищі, адаптуватися до новітніх викликів та використовувати сучасні інструменти аналітики. В Україні наразі триває процес формування системи освіти у сфері OSINT

[53] From Learners to Trainers: EUAM Ukraine trains trainers on OSINT within civil security agencies . URL: https://www.euam-ukraine.eu/news/from-learners-to-trainers-euam-ukraine-trains-trainers-on-osint-within-civil-security-agencies/;

EUAM: future Ukrainian police officers trained on international crime, OSINT, and European best practices. URL: https://euneighbourseast.eu/news/latest-news/euam-future-ukrainian-police-officers-trained-on-international-crime-osint-and-european-best-practices

та цифрової аналітики. Водночас підготовка фахівців у цій сфері залишається нерівномірною, а кадровий потенціал — недостатньо розвиненим, що створює системні обмеження у формуванні сталої екосистеми відкритої розвідки.[54]

На сьогодні національні заклади вищої освіти більш системно вводять курси або спецпредмети, пов'язані з аналізом відкритих джерел, кібербезпекою, інформаційною аналітикою, а також освітні програми, що включають елементи OSINT-освіти. Так, Національна академія Служби безпеки України, Національна академія внутрішніх справ, Київський національний університет імені Тараса Шевченка, Харківський національний університет внутрішніх справ, Інститут спеціального зв'язку та захисту інформації імені С.П. Корольова НТУУ «КПІ» пропонують курси з інформаційної аналітики, цифрової безпеки, кіберрозвідки, розвідки з відкритих джерел. Проте ці навчальні ініціативи здебільшого мають фрагментарний характер, а загальнонаціонального стандарту підготовки OSINT-фахівців наразі не існує.[55]

Ключовою проблемою залишається низька швидкість адаптації формальної освіти до практичних потреб сектору безпеки. В умовах динамічних змін освітня система поки що не встигає за запитами практики. Сучасне інформаційне середовище характеризується надзвичайною мінливістю, а інструменти OSINT постійно оновлюються. У зв'язку з цим, підготовка фахівців повинна враховувати не лише технічні аспекти (збір даних, геолокація, соціальна

---

[54] OSINT (Розвідка відкритих джерел) в екосистемі зв`язаних термінів. *Blogger.com.* URL: https://dss-bi.blogspot.com › 2019/01 › osint

[55] Академія СБУ підписала договір про співпрацю з OSINT-спільнотою Molfar. URL: https://nasbu.edu.ua/ua/news-1-8-297-akademiya-sbu-pidpisala-dogovir-pro-spivpracyu-z-osint-spilnotoyu-molfar?utm_source=chatgpt.com;

Освітньо-професійна програма «Аналітика даних». URL: https://fit.knu.ua/en/archives/9862?utm_source=chatgpt.com;

Тренінг з використання відкритих джерел інформації (OSINT) під час розслідування воєнних злочинів. URL: https://univd.edu.ua/uk/news/20024?utm_source=chatgpt.com

інженерія), але й міждисциплінарну складову (правові аспекти використання відкритих джерел, знання інформаційного права, етики, цифрової криміналістики, медіааналітики, геополітики, психології впливу та комунікаційних стратегій). Особливо актуальним є поєднання навичок OSINT із розумінням оперативної ситуації в умовах війни, знанням мов, геополітики та гібридної аналітики.

Наявна ситуація свідчить про необхідність цілеспрямованої державної політики у сфері розвитку освітньо-кадрового потенціалу OSINT. Зокрема, доцільним є:

– *розробка національного освітнього стандарту з підготовки фахівців з відкритої розвідки для сектору безпеки, правопорядку, стратегічних комунікацій*;

– *запровадження міжвідомчої платформи для підвищення кваліфікації OSINT-аналітиків із залученням представників державного та недержавного секторів*;

– *сприяння інтеграції формальної та неформальної освіти, зокрема шляхом підтримки OSINT-хабів, центрів відкритої аналітики, сертифікованих тренінгових програм*;

– *міжнародна співпраця у сфері підготовки кадрів, включно з академічною мобільністю, спільними проєктами з іноземними партнерами, впровадженням кращих практик НАТО та ЄС.*

Окремої уваги заслуговує роль громадянського суспільства у розвитку неформальної OSINT-освіти. Такі волонтерські ініціативи як InformNapalm[56], Molfar[57], OSINT-UA, Bihus.Info, Texty.org.ua та інші не лише займаються збором, аналізом та публікацією даних із відкритих джерел, а й активно формують середовище обміну знаннями. У межах цих спільнот діють внутрішні програми наставництва, проводяться відкриті тренінги, розробляються інструкції та гіди з використання OSINT-інструментів. У такий спосіб формується альтернативна платформа навчання,

[56] InformNapalm. URL: https://informnapalm.org/ua

[57] Molfar. URL: https://molfar.com

що суттєво підсилює кадровий потенціал у сфері цифрової аналітики. Волонтерські спільноти та громадянське суспільство також виступають неформальними освітніми майданчиками.

З огляду на системність викликів і стратегічне значення OSINT для національної безпеки, формування кадрового потенціалу має стати одним із пріоритетних напрямів політики держави в умовах тривалої гібридної війни. Саме від рівня підготовки аналітиків, їхнього доступу до знань і технологій залежить здатність України виявляти, прогнозувати та нейтралізовувати загрози інформаційного характеру, формувати сталу інформаційну екосистему та сприяти демократичному управлінню.

Разом із тим, відсутність національної системи сертифікації та стандартизації у підготовці OSINT-аналітиків є суттєвою перешкодою. У державному секторі наразі немає уніфікованих кваліфікаційних вимог до фахівців, кяі використовують відкриті джерела для розвідки або доказування. Це ускладнює формування професійної спільноти, перешкоджає мобільності кадрів та створює ризики неетичного або некомпетентного використання інформації. Потреба у стандартизації, сертифікації та професіоналізації залишається надзвичайно високою. Доцільно розробити національні освітні стандарти OSINT-підготовки для сектору безпеки та правопорядку, запровадити кваліфікаційні вимоги, створити платформу для постійного професійного розвитку аналітиків.

Україна демонструє значний прогрес у розвитку інституційної екосистеми OSINT. А саме формується широка мережа інструментів, методологій, спільнот та організацій, які разом сприяють збору, аналізу та використанню інформації з відкритих джерел та допомагають спеціалістам з OSINT у їхній роботі, під час якої забезпечується ефективний та надійний обмін знаннями та досвідом. Однак наступним кроком має стати перехід до системного управління, впровадження національної стратегії відкритої розвідки, створення мережі національних аналітичних

центрів, підвищення кваліфікації персоналу, правова інтеграція OSINT у систему кримінальної юстиції, безпеки та стратегічних комунікацій.[58]

Водночас можливим є виділення важливих напрямів подальшого розвитку інституційної спроможності:

- *Створення Національного центру відкритої розвідки (OSINT-Center).* Такий центр міг би стати координаційним органом із розробки стандартів, навчання кадрів, обміну даними, аналітичної підтримки сектору оборони та безпеки.
- *Прийняття Стратегії розвитку OSINT в Україні.* Необхідно затвердити стратегічний документ, який визначатиме роль OSINT у державному управлінні, безпеці, науці та правосудді.
- *Правова інтеграція OSINT.* Важливо внести зміни до КПК України, Законів України «Про інформацію», «Про національну безпеку», «Про розвідку», визначивши легітимний статус відкритої інформації в доказовій базі та оперативному реагуванні.
- *Міжвідомча взаємодія.* Запровадження постійно діючої міжвідомчої платформи з обміну OSINT-аналітикою за участю силових, розвідувальних, освітніх та громадських структур.
- *Підтримка громадських OSINT-ініціатив.* Фінансова, організаційна та правова підтримка волонтерських ініціатив, у тому числі через фонди безпеки, проєкти технічної допомоги, гранти.

Таким чином, інституційна спроможність України у сфері OSINT продовжує розвиватися на тлі війни як результат мобілізації наявних ресурсів, творчої адаптації до викликів та відкритості до партнерств. Проте для переходу до системного управління необхідно інтегрувати зусилля на стратегічному, правовому та кадровому рівнях.

---

[58] Уфімцева О.С. Використання OSINT в умовах збройної агресії РФ проти України. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права)* : у 2 т. : матеріали Міжнар.наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С.В. Ківалова. Одеса : Видавничий дім «Гельветика», 2022. Т. 1. С. 761–763.

Висновок

У сучасних умовах збройної агресії проти України відкриті джерела інформації набули принципово нового значення як в аспекті національної безпеки, так і в контексті інформаційного суверенітету. OSINT, що раніше розглядався як допоміжний аналітичний інструмент, трансформувався у самостійну розвідувальну дисципліну, спроможну не лише доповнювати традиційні форми розвідки, а й забезпечувати критичну підтримку процесів стратегічного планування, документування воєнних злочинів, протидії дезінформації та інформаційного впливу противника.

Під час повномасштабної війни роль OSINT значно зросла — завдяки швидкому доступу до відкритих даних, можливості геолокаційного аналізу, верифікації відео та фото, синтезу соціомедійного контенту, OSINT забезпечує оперативну обізнаність щодо подій на фронті та в тилу. При цьому демократичний характер OSINT, що дозволяє його використання як державними органами, так і волонтерами, журналістами, дослідниками, створює потужний горизонтальний ресурс національного спротиву.

Водночас із перевагами, стрімке поширення OSINT породжує низку серйозних викликів: витоки критичної інформації, свідоме або несвідоме розкриття дислокацій військових підрозділів, логістичних маршрутів, персональних даних, підвищують вразливість країни до кібератак, фізичних диверсій та інформаційно-психологічних операцій. Відсутність належного регламентування використання OSINT, дефіцит цифрової гігієни серед населення, етичні та правові колізії — все це створює ризики як для державної, так і для індивідуальної безпеки.

В умовах воєнного стану нагальною є потреба у створенні цілісної системи управління та захисту процесів розвідки з відкритих джерел. Вона має включати правове врегулювання обігу відкритих даних, розвиток інституційної спроможності аналітичних підрозділів, підвищення рівня інформаційної гігієни та формування

культури відповідального ставлення до інформації серед населення. Не менш важливими залишаються питання міжвідомчої взаємодії, технологічної модернізації та поглиблення міжнародної співпраці.

Український досвід переконливо свідчить: для ефективного застосування OSINT необхідний перехід від фрагментарного до системного підходу, який передбачає розробку стратегії державної політики у сфері розвідки з відкритих джерел, визначення чітких меж її правового статусу, створення спеціалізованих платформ і мультидисциплінарних команд.

Особливої уваги потребує формування етичної культури поводження з відкритою інформацією: навіть доступні дані можуть становити загрозу, якщо вони неконтрольовано публікуються або аналізуються без урахування безпекового контексту. Відтак, OSINT повинен розвиватися як інструмент з високим рівнем професіоналізму, стандартизації та міжвідомчої координації.

Таким чином, OSINT — це не лише технологія чи аналітичний інструмент. Це — складова цифрової безпеки, елемент гібридного опору, основа для сучасної моделі безпекового мислення. Його ефективне використання потребує балансу між відкритістю інформації та безпекою, що є основою стійкості держави у сучасних умовах. Разом з тим, продуктивне застосування OSINT можливе лише за умови поєднання правових гарантій, освітніх зусиль, технологічної спроможності та стратегічного бачення держави. Досвід України показав, що розвідка з відкритих джерел здатна забезпечити оперативність, точність та масштабність аналізу, доповнюючи традиційні методи розвідки. Досвід України у цьому напрямі є унікальним і може стати основою для формування новітніх стандартів розвідки у XXI сторіччі.

Наукове видання

ПРАВОВЕ РЕГУЛЮВАННЯ ДОТРИМАННЯ ПРАВ І СВОБОД ЛЮДИНИ ТА ГРОМАДЯНИНА В УМОВАХ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ

Колективна монографія

Верстка	*Н. Ковальчук*
Обкладинка	*А. Юдашкіна*
Технічне редагування	*О. Гринюк*

ЮРИДИКА
ВИДАВНИЦТВО

Підписано до друку 07.10.2025 р. Формат 60x84/16.
Папір офсетний. Гарнітура Warnock. Цифровий друк.
Ум. друк. арк. 48,83. Наклад 300.
Замовлення № 085м-1125.
Віддруковано з готового оригінал-макета.

Видавництво і друкарня – Видавництво «Юридика»
65101, Україна, м. Одеса, вул. Інглезі, 6/1
Телефони: +38 (095) 934 48 28, +38 (097) 723 06 08
E-mail: mailbox@juridica.od.ua
Свідоцтво суб'єкта видавничої справи
ДК № 7653 від 18.08.2022 р.